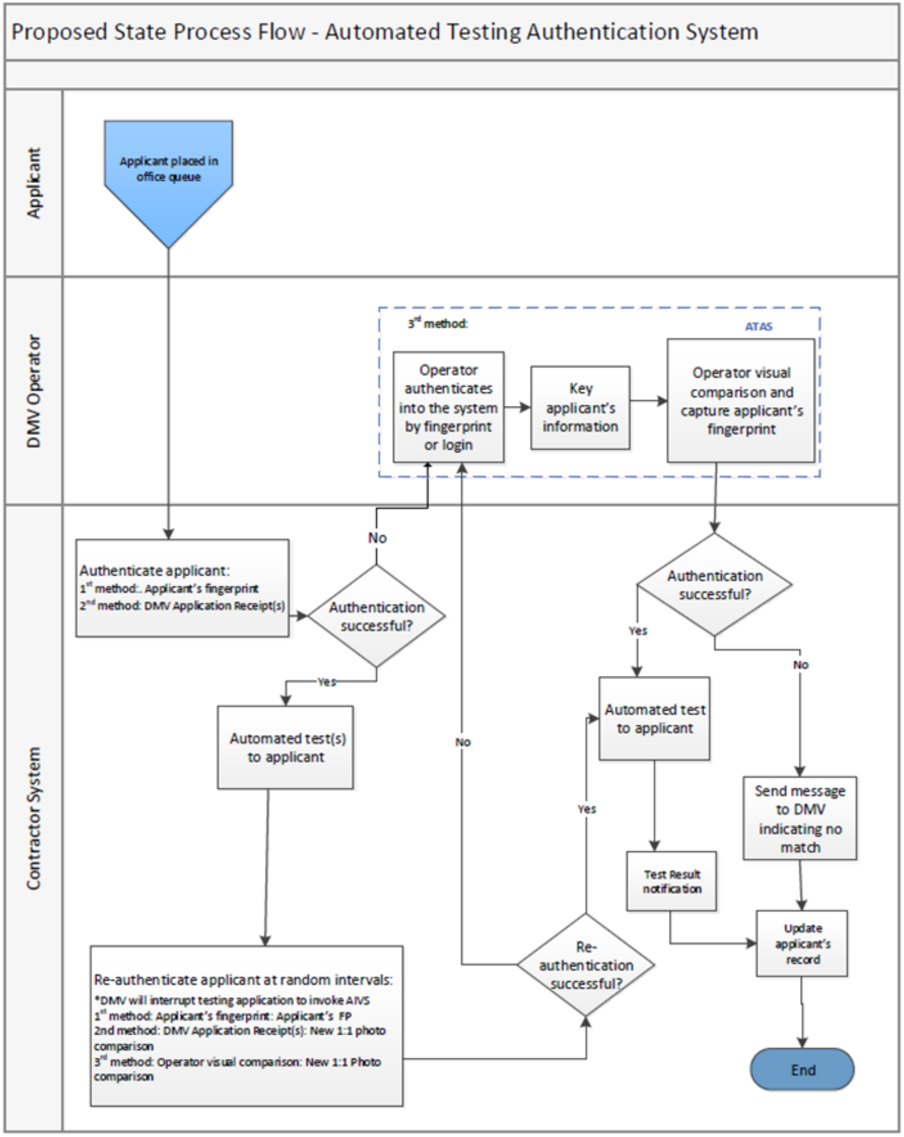
Mandatory Optional Solutions and Systems

A description of the mandatory optional features that DMV is considering to be part of AIVS for this solicitation.

1. Automated Testing Authentication System (ATAS)

The DMV administers tests to applicants in the field office using the Automated Testing Terminal (ATT) and relies primarily on the applicant's fingerprint to verify his/her identity through a 1:few fingerprint comparison. The AIVS shall utilize the ATT to more thoroughly authenticate the identity of an applicant and ensure that the applicant is the same individual taking the test. The high level process flow is as follows:

Proposed Automated Testing Authentication System


Proposed State Process Flow - Automated Testing Authentication System
Applicant
DMV Operator
Contractor System
Applicant placed in office queue
3rd method:
ATAS
Operator authenticates into the system by fingerprint or login
Key applicant's information
Operator visual comparison and capture applicant's fingerprint
Authenticate applicant:
1st method:. Applicant's fingerprint
2nd method: DMV Application Receipt(s)
Authentication successful?
No
Yes
Automated test(s) to applicant
Authentication successful?
Yes
No
Automated test to applicant
No
Yes
Send message to DMV indicating no match
Test Result notification
Update applicant's record
Re-authentication successful?
Re-authenticate applicant at random intervals:
*DMV will interrupt testing application to invoke AIVS
1st method: Applicant's fingerprint: Applicant's FP
2nd method: DMV Application Receipt(s): New 1:1 photo comparison
3rd method: Operator visual comparison: New 1:1 Photo comparison
End

The AIVS will initially facilitate this authentication by matching an applicant's fingerprint to the individual's record in the Office Queue. If the fingerprint match is not found, the applicant will scan the barcode from the DMV application receipt(s). This is a mandatory requirement for Automated Testing Terminals.

The DMV is considering, if the barcode scan does not find a match, the operator will log into the system using his/her own fingerprint and search for the applicant using the applicant last name and DL number. The operator will then visually compare the applicant against the photo of record to verify his/her identity.

If the applicant record is successfully identified in the Office Queue using one of the preceding matching approaches, the AIVS shall integrate the applicant's data with the ATT to display the photo on record, authorizing the applicant to take the test. The photo of record will display on the test screen throughout the test process. If the operator cannot confirm a match, the process is stopped and the AIVS would send a notification to the DMV, indicating no match.

As an extra layer of security, the AIVS shall integrate a random applicant authentication that will require the applicant to revalidate his/her identity. The validation approach will be dependent on how the applicant was initially verified into the testing system. These business rules are identified as follows:

If the applicant logged in with a fingerprint, the solution shall require the fingerprint to be re-validated. If that process fails, the operator must log into the system and visually validate the applicant against the photo of record, or the test is stopped. If the operator cannot confirm a match, the process is stopped and the AIVS would send a notification to the DMV, indicating no match.

If the applicant logged in with a barcode scan of the DMV application receipt, the system will notify the applicant that a new photo will be taken with the ATAS camera at the terminal. The system will then perform a 1:1 electronic photo comparison against the photo of record. If that process fails, the operator must log into the system and visually validate the applicant against the photo of record and capture the applicant's fingerprint, or the test is stopped. If the operator cannot confirm a match, the process is stopped and the AIVS would send a notification to the DMV, indicating no match.

If the operator had to initially visually verify the applicant, the system will notify the applicant that a new photo will be taken at the terminal, and the system will then perform a 1:1 electronic photo comparison against the photo of record. If that process fails, the operator must log into the system and visually validate the applicant against the photo of record and capture the applicant's fingerprint, or the test is stopped. If the operator cannot confirm a match, the process is stopped and the AIVS would send a notification to the DMV, indicating no match.

2. DRIVE TEST AUTHENTICATION SYSTEM (DTAS)
The AIVS shall have the functionality to incorporate the use of mobile devices for DMV operators (e.g., drive test employees) to provide a means to authenticate and authorize applicants for the drive test while outside of DMV FOs. This process utilizes the same 1:1 fingerprint comparison software and visual photo comparison used within the FO and will be available for a drive test.

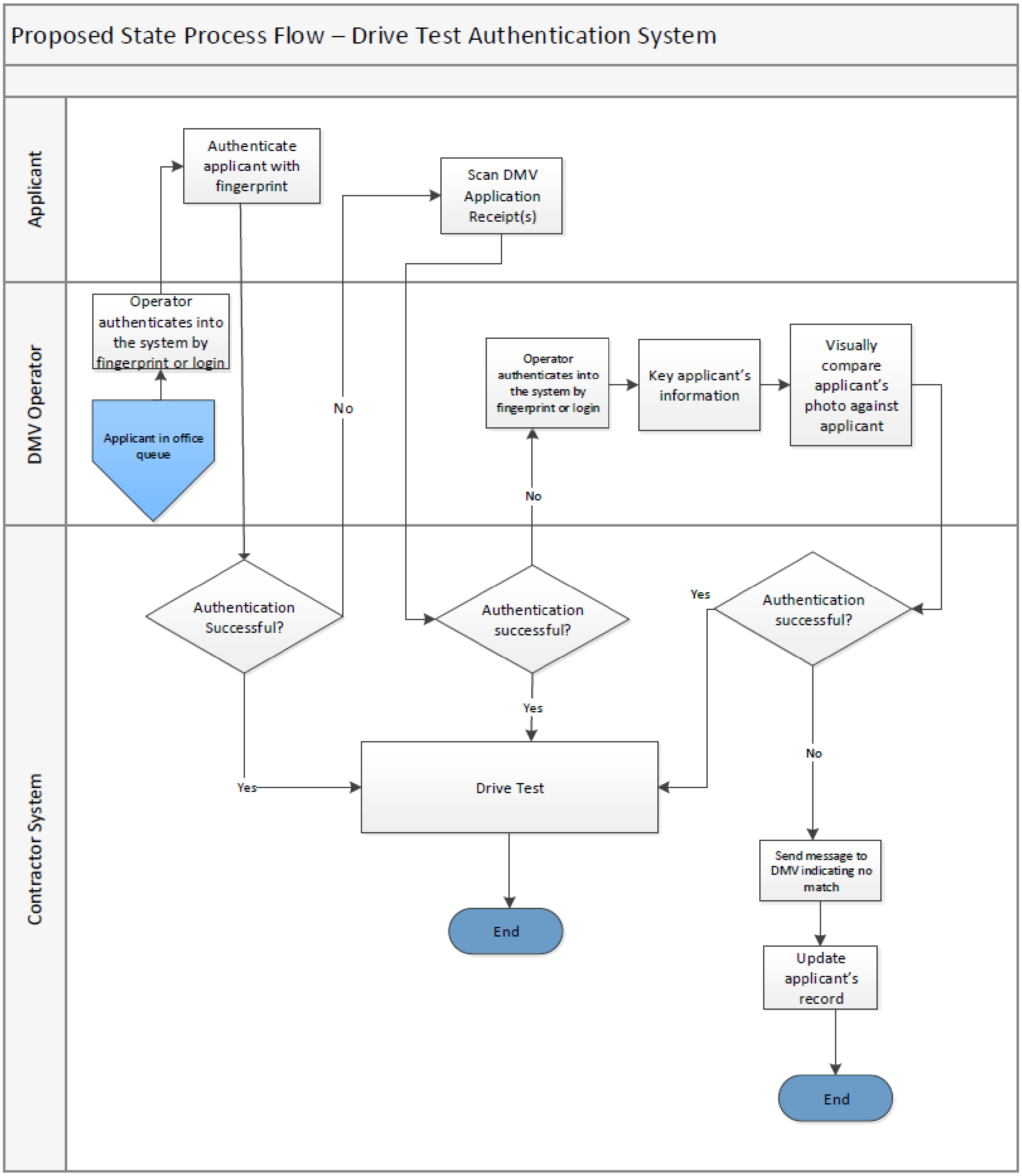
Drive Test Authentication System (DTAS) shall leverage cellular communications, allowing the DMV operator to authenticate an applicant's identity while physically positioned outside of the DMV FO building. The operator will log into DTAS using his/her fingerprint or his/her operator ID and password. DTAS will scan the applicant's fingerprint to identify and match the individual's record from the Office Queue.

If the fingerprint matches successfully and identifies an applicant from the Office Queue, the AIVS shall prompt the operator to validate the applicant's photo to continue and select the applicant from the queue.

If fingerprint matching cannot identify the applicant from the Office Queue, the DMV operator may utilize the barcode from the applicant's photo receipt to identify the record in the queue.

If the operator cannot match the applicant to the photo, the process is stopped and the AIVS would send a notification to the DMV, indicating no match.

Proposed State Process Flow – Drive Test Authentication System


Proposed State Process Flow – Drive Test Authentication System
Applicant
DMV Operator
Contractor System
Authenticate applicant with fingerprint
Scan DMV Application Receipt(s)
Operator authenticates into the system by fingerprint or login
Applicant in office queue
No
Operator authenticates into the system by fingerprint or login
Key applicant's information
Visually compare applicant's photo against applicant
No
Authentication Successful?
Authentication successful?
Yes
Authentication successful?
Yes
Yes
Drive Test
No
Send message to DMV indicating no match
Update applicant's record
End
End

3. FACIAL RECOGNITION – Card Issuance

The DMV is considering, the use of facial recognition biometrics as an optional approach for authenticating the identity of an applicant during the card issuance process. When a match is found for a one to many (1:N) FR search, a 1:F FP comparison shall be performed on records identified. If any identified record(s) matches on the 1:F FP comparison, the Firm shall not issue the card. The card is not produced and the matching record's data is sent to DMV.

The AIVS shall incorporate a Facial Recognition (FR) Investigative Workstation. This workstation shall provide functionality for operators to identify and investigate duplicate IDSs by utilizing 1:FR and 1:N search functionality for a specific record. The functions of the FR Investigative Workstation may be allowed to reside on the Retrieval Workstations identified as part of the AIVS.

4. MAILING SOLUTION - DMV DELIVERY

The DMV mailing system is currently provided by Pitney Bowes and is operated by DMV staff at the DMV HQ Production Mail Center. The DMV is considering a Firm provided Mailing Solution that includes a specialized, custom-built mailing machine, along with service, that has the capability to process cards, envelopes, forms, and inserts. The Mailing Solution will utilize similar processes as the current mailing environment but will scan barcodes on the card instead of the card magnetic stripe. Cards that do not match carrier forms, or that cannot be read, will automatically be diverted to prevent slowdown of mailing operations. The mailing machine must be able to combine all input consumables (cards, envelopes, specific forms, and inserts) into a mailable flat compliant with United States Postal Service (USPS) guidelines. The flats are weighed and metered, and are 100% ready to mail from the DMV HQ processing location to applicants across the State and abroad (outside of California in another state, country, or other location) as needed.

The Mailing Solution shall read data on the TIS file and will be required to update the TIS file with "date mailed" information. Once a batch of cards has been successfully and accurately processed for mailing, the TIS file will be removed from the Mailing Solution and returned to the appropriate DMV HQ unit for updating of the "date mailed" field in TIS as well as the DRM.

The Mailing Solution must include card counting machines for use by DMV staff through the card mailing process.

5. MAILING SOLUTION – FIRM MAILING

At the State's discretion, the Firm must mail out the DLIDSP cards to the applicants. This process would require the Firm to provide data that indicates, at a minimum, when the cards were processed for mailing. In addition, the Firm would be responsible for the consumable products that are needed for any card mailers and associated printing needs along with the postage required.

6. VIRTUAL BACKDROP FOR IMAGE CAPTURE PROCESSING-CENTRALIZED

In lieu of the physical ICS backdrop described in the current environment, DMV is considering virtual backdrop alternatives to allow for improved photo capture process efficiency. This solution allows for the use of a centralized office camera. All other ICS specifications for the camera and associated application remain the same unless otherwise noted.

7. VIRTUAL BACKDROP FOR IMAGE CAPTURE PROCESSING-DECENTRALIZED

In lieu of the physical ICS backdrop described in the current environment, DMV is considering virtual backdrop alternatives to allow for improved photo capture process efficiency. This solution allows for the use of multiple cameras, located at the technician windows. All other ICS specifications for the camera and associated application remain the same unless otherwise noted.

8. APPLICANT SERVICES

A system for use by applicants when applying for a DLIDSP card through a customer facing application that performs tasks related to identity credentials, document image collection and authentication (e.g. legal presence documents), and uploads the document images for long term storage. This is similar to the DMV Express system identified in Exhibit W, Bidder's Library, Current Processes and Environment.

9. VIRTUAL TESTING/PROCTORING

A system that provides automated, remote proctoring of driver license knowledge tests that is integrated with the identify verification and test delivery platforms used by the DMV. Capabilities include, but are not limited to, real-time facial recognition/verification, on-demand testing, 24/7 technical support, restricting abilities of browser and desktop, restricting access to knowledge testing environment only, audio and video capture of desktop and testing environment, and artificial intelligence analysis of captured data.

10. MOBILE TECHNICIAN
A system for capturing and comparing applicant biometrics and supporting application documents using a mobile tablet and peripheral devices. Captured data and images must be transferred over a secure connection to a secure image server location without compromising the data security on the tablet and devices on which the images are captured. Capabilities are included but not limited to photo capture and data extraction from California DLIDSP cards, photo capture and data extraction from supporting application documents, capturing fingerprint and signatures, transferring data and images to an image server, transferring fingerprint images, manual data capturing, and generating a unique transaction code that may be used to download temporary travel identification.

11. DIGITAL DLIDSP CARD
A system which allows for the transmission and display of a California DLIDSP Card on a mobile device, such as a cell phone, for the card holder. This system may not replace the physical DLIDSP Card but may be an additional service.